UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/483,164	01/14/2000	Daniel Jay Thomsen	105.174US1	8029

21186 7590 03/16/2005

SCHWEGMAN, LUNDBERG, WOESSNER & KLUTH, P.A.
P.O. BOX 2938
MINNEAPOLIS, MN 55402

EXAMINER	
SIMITOSKI, MICHAEL J	

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 03/16/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/483,164	THOMSEN ET AL.	
	Examiner	Art Unit	
	Michael J Simitoski	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03 June 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-35* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-35* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *14 December 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. The response of 3/22/2004 was received and considered.

2. As per the election of 7/12/2004, claims 36-38 are cancelled.

3. Claims 1-35 are pending.

4. Claims 1-35 are rejected.

5. This Office Action is made non-final.

6. The objections to claims 15, 17, 20 & 29 are withdrawn.

7. The corrections to the disclosure, presented in a paper dated 3/22/2004, pp. 2-4 are accepted and therefore the objections to the disclosure are withdrawn.

Response to Arguments

8. Applicant's arguments regarding the Thomsen reference have been fully considered but they are not persuasive.

9. Applicant's response (p. 12, last ¶ - p. 13, ¶3) argues that Thomsen does not describe (1) the use of semantic layers to combine keys into key chains, (2) why or how one would encapsulate key chains as keys within a semantic layer or why or how one would pass the encapsulated chains to the next semantic layer, (3) a plurality of semantic layers or a user interface for defining a security policy as a function of keys received from lower semantic layers as described by Applicant and claimed in claims 6-10 and (4) a tool for manipulating the RBAC model as described by Applicant and claimed in claims 11-13.

Regarding (1), Thomsen discloses semantic layers (§1, ¶1 & Fig. 1) to combine keys into key chains (Fig. 1 & Fig. 2),

Regarding (2), Thomsen discloses encapsulating key chains (for example "Doctor" and "Nurse", Fig. 2) as keys ("Health Care Provider", Fig. 2) within a semantic layer (application) (Fig. 1) and passing the encapsulated key chains to the next semantic layer (enterprise) (Fig. 1, §2 ¶3 & §2.7),

Regarding (3), Thomsen discloses a plurality of semantic layers (Fig. 1) and a user interface/policy tool (§3) for defining a security policy as a function of keys received from lower semantic layers (§3.1 ¶1), and

Regarding (4), Thomsen discloses a tool/NAPOLEAN for manipulating the RBAC model (creating new application keys) (Fig. 4 & §3.1, "Specifying Policy").

10. Applicant's arguments, see paper dated 3/22/2004, p. 12, ¶6 – p.14, ¶4, with respect to the rejection(s)of claim(s) 1-35 under Crall (35 U.S.C. 102 and 103) have been fully considered, but are considered moot in view of new ground(s) of rejection is made in view of new interpretation of the previously applied Sandhu reference.

11. Regarding the semantic layers in general (as described in the Sandhu reference used herein), Sandhu discloses the following concepts: (1) Permissions are encapsulated into abilities (which can contain other abilities), and (2) abilities are assigned, with users, to roles (which can contain other roles). Therefore, a semantic layer can be thought of as a particular layer abstracting permissions into abilities, a layer abstracting roles to different users, or some combination of the two. As an example of the first, *save* and *write* can be encapsulated into (*edit*) and *open* and *view* can be encapsulated into (*read*) where *edit* and *read* are abilities. This can be extended where an ability called *interact* is assigned the *edit* and *read* abilities – creating

semantic layers of permissions only. As an example of the second, *editor* and *reader* could be roles encapsulating *edit* and *read* abilities. Further, a role *manager* could encapsulate the roles *reader* and *editor*, allowing the manager to inherit the permissions of the two – creating semantic layers of roles. Since roles can be assigned permissions, any combination of these two is possible. The rejections follow.

Claim Rejections - 35 USC § 101

12. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

13. Claims 1 & 3-31 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. The invention of the claims is not tangibly embodied.

Claim Rejections - 35 USC § 112

14. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

15. Claims 12-13 rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Regarding claims 12 & 13, the claims are method claims depending from a system claim and it is unclear how to interpret the claims as a result.

Claim Rejections - 35 USC § 102

16. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

17. Claims 1-3, 5-8, 11-19, 21-28, 30 & 32-34 are rejected under 35 U.S.C. 102(a) as being anticipated by printed publication "Role Based Access Control Framework for Network Enterprises" by Thomsen, O'Brien and Bogle (Thomsen).

Regarding claims 1, 6, 11, 13-16, 22-24, 30, & 32-34, Thomsen discloses encapsulating security mechanism application specific information for each security mechanism/methods (Fig. 1 & §2.4), wherein encapsulating includes forming a key for each security mechanism (Fig. 2 & §2.4), combining keys to form key chains (Figs. 1 & 2), encapsulating key chains as keys (for example "Doctor" and "Nurse", Fig. 2) as keys ("Health Care Provider", Fig. 2) and passing the key chain keys to another semantic layer (from application to enterprise) (§2.5), defining the security policy, wherein defining includes forming key chains from keys and associating users with key chains (§2.6-§2.7), translating the security policy (p. 7, last ¶2) and exporting the translated security policy to the security mechanisms (to CORBA using ADAGE (p. 8, ¶1) and enforcing the security policy via the security mechanisms/CORBA (p. 8, ¶1).

Regarding claim 2, Thomsen discloses a distributed computer network (§1.1).

Regarding claim 3, Thomsen discloses the security mechanisms being heterogeneous (p. 8, §3.2).

Regarding claims 5 & 7, Thomsen discloses defining the policy using a graphic user interface/NAPOLEAN policy tool (Fig. 4 & §3.1, "Specifying Policy").

Regarding claim 8, Thomsen discloses a role-based access control model (§1.2).

Regarding claim 12, Thomsen discloses a static application policy layer (application), one or more semantic policy layers (key chaining, Fig. 2) and a dynamic policy layer (enterprise) (Fig. 1).

Regarding claims 17 & 25-26, Thomsen discloses associating a constraint with a key (§2.3) where the constraint must be satisfied before access to a computer resource governed by the key chain is granted (§2.3 ¶1).

Regarding claims 18 & 27, Thomsen discloses grouping methods/objects into handles and handles into keys (Fig. 1).

Regarding claims 19 & 28, Thomsen discloses each key chain including handles for different computer resources (§2.2 ¶4).

18. Claims 1-35 are rejected under 35 U.S.C. 102(a) as being anticipated by printed publication "Napoleon Network Application Policy Environment" by Thomsen, O'Brien and Bogle (Thomsen). Thomsen discloses using an application layer, semantic layers and a local layer (Fig. 2 & §2), encapsulating keys into key chains, and exporting the key chains to the next layer (§2 & Fig. 2), combining methods into handles, handles into keys and keys into key chains (Fig. 3), and adding constraints to the key chains at each layer (Fig. 4), assigning users to key

chains (§2.3), using a user interface to manage the RBAC policy (§3) and translating the policy to the security mechanisms (§4).

19. Claims 1-4 & 32 rejected under 35 U.S.C. 102(e) as being anticipated by "The ARBAC97 Model for Role-Based Administration of Roles" by Sandhu et al. (Sandhu).

Regarding claim 1, 3 & 32, Sandhu discloses encapsulating security mechanism application specific information/permissions for each security mechanism/permission (p. 122, §5), wherein encapsulating includes forming a key/ability for each security mechanism/permission, combining keys/abilities to form key chains/abilities, encapsulating key chains/abilities as keys/abilities (p. 122, §5) and passing the key chain keys/abilities to another semantic layer/UP-Roles (p. 122, §5), defining the security policy/UP-Roles (p. 122, §5), wherein defining includes forming key chains from keys/abilities and associating users with key chains/abilities (p. 122, §5), translating the security policy/UP-Roles and exporting the translated security policy to the security mechanisms, and enforcing the security policy via the security mechanisms (p. 107, ¶5 & Fig. 1).

Regarding claim 2, Sandhu discloses distributed computer networks/enterprise-wide systems (p. 106, ¶4).

Regarding claim 4, Sandhu discloses UP-Roles, containing both abstracted abilities and permissions (p. 122, §5). If a new role is to be created, the next layer (abilities/users) is drilled to/accessed to combine the necessary elements.

Claim Rejections - 35 USC § 103

20. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

21. Claims 5-17, 21-26, 30 & 33-34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sandhu, as applied to claim 1 above, in further view of "Issues in the Design of Secure Authorization Service for Distributed Applications" by Varadharajan, Pato and Crall (Crall).

Regarding claim 5, Sandhu discloses a system, as described above, but lacks a graphical user interface. However, Crall teaches that a graphical user interface makes it easy for administrators to manage large numbers of users with consistent policies across applications (p. 874). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use a graphical user interface to define the security policy. One of ordinary skill in the art would have been motivated to perform such a modification to make it easy for administrators to manage large numbers of users with consistent policies across applications, as taught by Crall (p. 874).

Regarding claim 6-8, Sandhu discloses a plurality of security mechanisms/permissions, a plurality of semantic layers (UP-Roles, abilities, permissions) (p. 122, §5), wherein the first semantic layer combines keys/abilities, wherein each key encapsulates security mechanism application specific information for a security mechanism (permissions for resources) (p. 122, §5). Sandhu lacks an explicit translator for translating the security policy to the security

mechanisms and lacks a user interface. However, Crall discloses an "Authorization Server", which employs an interface to make it easy for administrators to manage users (p. 874). In disclosing the physical implementation that Sandhu lacks, Crall further discloses that authorization checks result from the security mechanisms/authorization mechanisms (p. 876, §2.4) when changes are made, translation occurs to keep the authorization database up to date (p. 878, ¶1). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to include a translator to translate the security policy to the security mechanisms and to include a user interface. One of ordinary skill in the art would have been motivated to perform such a modification to implement Sandhu's invention, in order to keep the authorization database up to date and to allow administrators to manage large groups of users, as taught by Crall (p. 874, p. 876, §2.4 & p. 878, ¶1).

Regarding claim 9, Sandhu discloses the semantic layers (role hierarchy) organized in a POSET/partial order to facilitate inheritance.

Regarding claim 10, Sandhu discloses that new key chains/abilities can be formed by any combinations of abilities and permissions (p. 122, §5), but lacks a user interface. However, Crall teaches that a graphical user interface makes it easy for administrators to manage large numbers of users with consistent policies across applications (p. 874). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use a graphical user interface to define the security policy. One of ordinary skill in the art would have been motivated to perform such a modification to make it easy for administrators to manage large numbers of users with consistent policies across applications, as taught by Crall (p. 874).

Regarding claim 11, Sandhu discloses a model comprising one or more semantic layers/roles for defining different security policies (p. 122, §5) and constraints (p. 108, ¶1) for each type of user, but lacks a tool for manipulating the model and lacks a translator for translating security policies from the model to security mechanisms in one or more computer resources. However, Crall discloses an "Authorization Server", which employs an interface to make it easy for administrators to manage users (p. 874). In disclosing the physical implementation that Sandhu lacks, Crall further discloses that authorization checks result from the security mechanisms/authorization mechanisms (p. 876, §2.4) when changes are made, translation occurs to keep the authorization database up to date (p. 878, ¶1). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to include a translator to translate the security policy to the security mechanisms and to include a tool for manipulating the model. One of ordinary skill in the art would have been motivated to perform such a modification to implement Sandhu's invention, in order to keep the authorization database up to date and to allow administrators to manage large groups of users, as taught by Crall (p. 874, p. 876, §2.4 & p. 878, ¶1).

Regarding claim 12, Sandhu discloses different semantic layers/roles, but lacks a static application policy layer, and a dynamic local policy layer. However, Crall teaches that security information is both static and dynamic (prone to state changes) (p. 875, §2.2). Crall further teaches that it is important to differentiate the static and dynamic security information so that it can be managed differently (p. 875, §2.2). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to include dynamic local and static

application policy layers. One of ordinary skill in the art would have been motivated to perform such a modification to allow separate management, as taught by Crall (p. 875, §2.2).

Regarding claims 13-14, 21-22, 30 & 33-34, Sandhu discloses defining an application policy layer (p. 106, ¶1) and a plurality of semantic policy layers, including a first semantic policy layer and a second semantic policy layer (role x and role y, p. 107, ¶5 (example)), encapsulating a set of access rights/permissions for a computer resource as a key/ability, combining keys to form one or more key chains/ability within the application policy layer, exporting key chains in the application policy layer as a key/ability, importing at least one key from the application policy layer into the first semantic policy layer, combining one or more keys/abilities in the first semantic policy layer to form a key chain/ability, exporting key chains in the first semantic policy layer as keys, importing at least one key/ability into the second semantic policy layer, combining one or more keys/abilities in the second semantic policy layer to form a key chain, exporting key chains/abilities in the second semantic policy layer as keys, importing at least one key from the second semantic policy layer to a local policy layer (UP-roles), combining one or more keys in the local policy layer to form one or more local policy key chains/abilities, and assigning users to local policy key chains/abilities in the local policy layer (UP-roles) (p. 122, §5). Sandhu does not disclose explicitly the combining of permissions+abilities and abilities+abilities, as described in the claim, but merely discloses that the purpose of the model is to allow this for the purpose of treating permissions as single units (p. 122, §5) (Sandhu describes the model, not an implementation of the model). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to specifically encapsulate keys into key chains and export the key chains as keys for each

of the layers so that administrators can treat permissions for users as single units, as taught by Sandhu (p. 122, §5).

Regarding claims 15, 16, 23 & 24, Sandhu discloses combining one or more keys/abilities to form a key chain (also an ability) includes combining a key chain/ability with the one or more keys/abilities to form another key chain/ability (p. 122, §5).

Regarding claims 17, 25 & 26, Sandhu discloses placing constraints on the key chains/abilities where the constraint must be satisfied before access to a computer resource governed by the key chain/ability is granted (p. 108). Sandhu teaches that this is done to apply the well-known business practice of separation of duties (p. 108).

22. Claims 31 & 35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sandhu in view of Crall in further view of "The Role Graph Model and Conflict of Interest" by Nyanchama et al. (Nyanchama). Sandhu discloses a model, as described above, which uses partial ordering (p. 107, §2) but lacks adding and deleting keys from a role hierarchy graph. However, Nyanchama teaches that role graphs provide a way of visualizing the interactions among roles and their seniors and juniors (p. 4, ¶1). Further, Crall teaches that a graphical user interface makes it easy for administrators to manage large numbers of users with consistent policies across applications (p. 874). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to enable a user to add and delete roles using a role hierarchy graph. One of ordinary skill in the art would have been motivated to perform such a modification to visualize the interactions among roles and their seniors and

juniors, as taught by Nyanchama (p. 4, ¶1) and to make it easy for administrators to manage large numbers of users with consistent policies across applications, as taught by Crall (p. 874).

Conclusion

23. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael J. Simitoski whose telephone number is (571) 272-3841. The examiner can normally be reached on Monday - Thursday, 6:45 a.m. - 4:15 p.m.. The examiner can also be reached on alternate Fridays from 6:45 a.m. – 3:15 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached at (571) 272-3838.

Any response to this action should be mailed to:
Commissioner of Patents and Trademarks
Washington, DC 20231
Or faxed to:
(703)746-7239 (for formal communications intended for entry)
Or:
(571)273-3841 (Examiner's fax, for informal or draft communications, please label "PROPOSED" or "DRAFT")

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (571) 272-2100.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MJS
March 2, 2005

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100